CTS Advisory Council

Office 365
Tenant Design

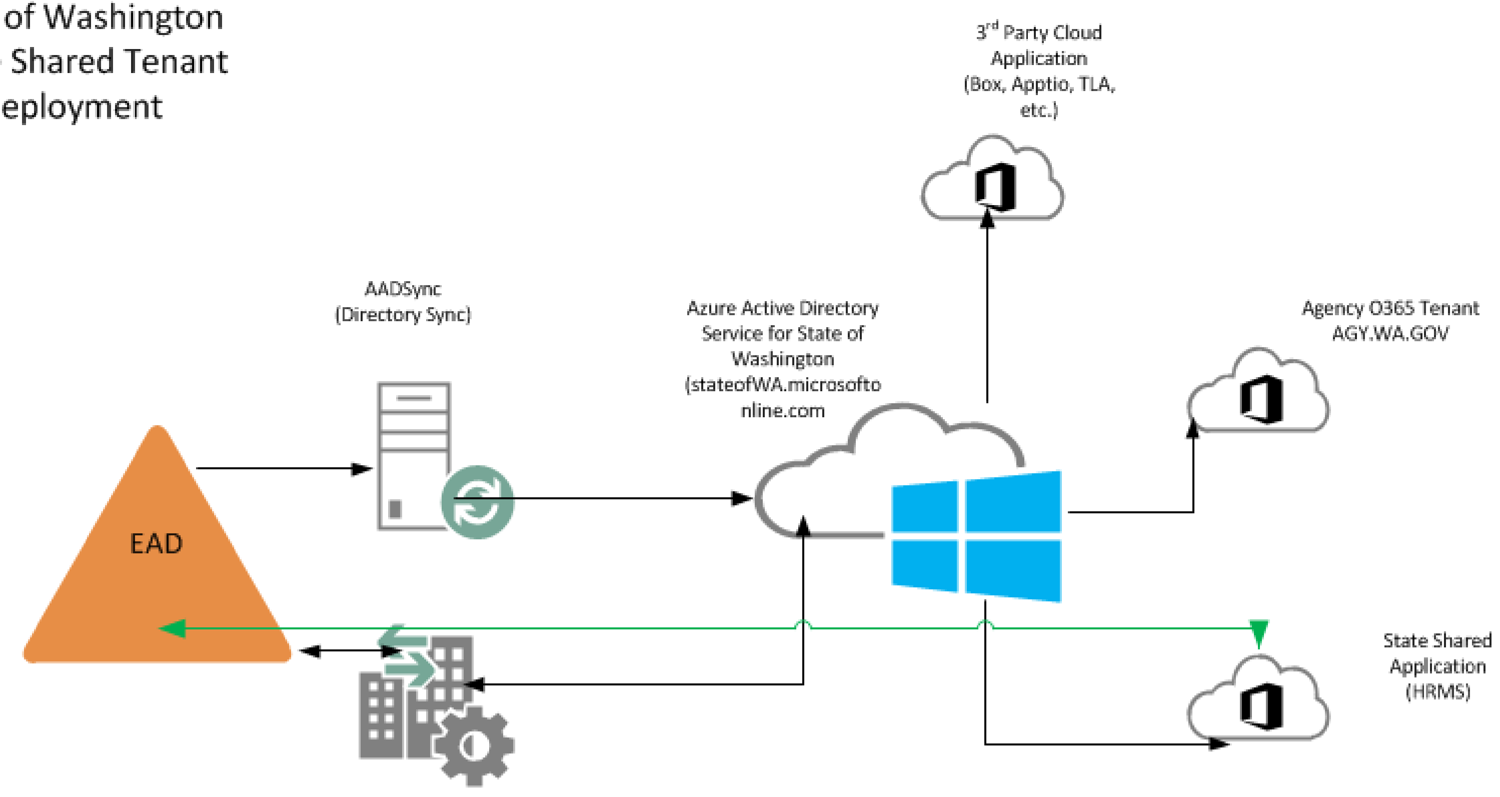
November 2014

Design Considerations

Requirement	Design Choice	Benefits
Secure Implementation	1) Single instance of Azure Active Directory 2) Government Tenant	1) Limits exposure of state identities; provides single identity store for federation to cloud services 2) Meets certification and segregation needs of majority of state agencies
Minimize Costs	Single Shared Tenant	Single ADFS/AADSync Servers; avoids duplicate licensing for collaboration between agencies.
Future Migration to O365	Single Shared Tenant	Only one hybrid Exchange or Lync connection allowed to only one tenant
Delegated Administration	Single Shared AAD	Administrative Units being developed for agency delegation
Support Collaborative Use	Single Shared Tenant	Allows for single address book; shared cloud applications and internal applications from same directory; minimize duplicate licensing

O365 Single Tenant Design

State of Washington
Single Shared Tenant
Deployment



3rd Party Cloud Application (Box, Apptio, TLA, etc.)

AADSync (Directory Sync)

Azure Active Directory Service for State of Washington (stateofWA.microsoftonline.com

Agency O365 Tenant AGY.WA.GOV

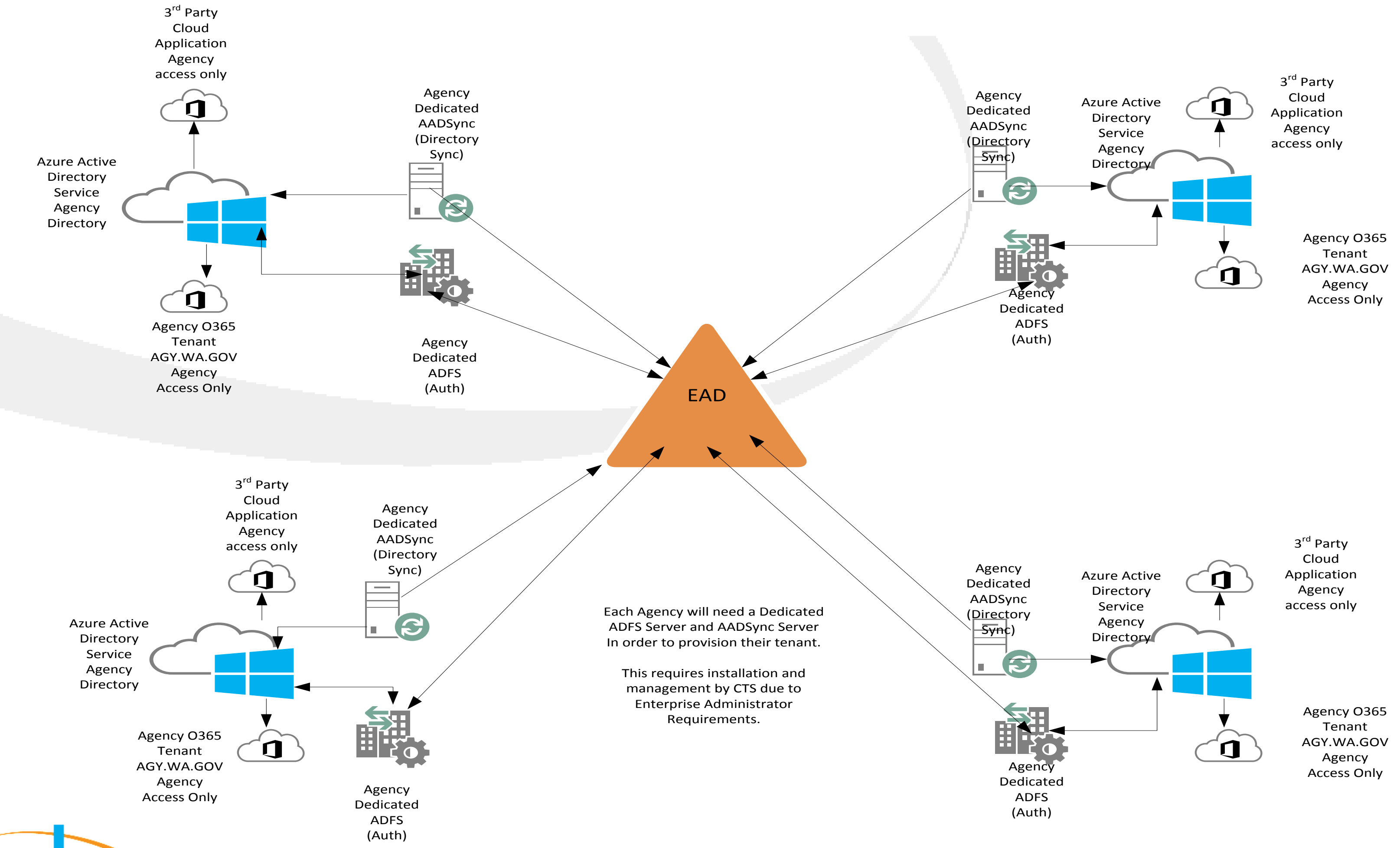
EAD

State Shared Application (HRMS)

Active Directory Federation Services (Authentication)

Current ADFS infrastructure includes redundancy in Spokane and ADFS Proxy for external authentication.

O365 Multi-Tenant Design



3rd Party Cloud Application Agency access only

Azure Active Directory Service Agency Directory

Agency Dedicated AADSync (Directory Sync)

Agency O365 Tenant AGY.WA.GOV Agency Access Only

Agency Dedicated ADFS (Auth)

Agency Dedicated AADSync (Directory Sync)

Azure Active Directory Service Agency Directory

3rd Party Cloud Application Agency access only

Agency Dedicated ADFS (Auth)

Agency O365 Tenant AGY.WA.GOV Agency Access Only

EAD

3rd Party Cloud Application Agency access only

Agency Dedicated AADSync (Directory Sync)

Azure Active Directory Service Agency Directory

Agency O365 Tenant AGY.WA.GOV Agency Access Only

Agency Dedicated ADFS (Auth)

Agency Dedicated AADSync (Directory Sync)

Azure Active Directory Service Agency Directory

3rd Party Cloud Application Agency access only

Agency Dedicated ADFS (Auth)

Agency O365 Tenant AGY.WA.GOV Agency Access Only

Each Agency will need a Dedicated ADFS Server and AADSync Server In order to provision their tenant.

This requires installation and management by CTS due to Enterprise Administrator Requirements.

Estimated Costs of ADFS/AADSync Environment per Tenant

Minimum Requirement	**High Availability** **(One ADFS and Proxy in Spokane; no HA option for AADSync at this time)**
1 ADFS Server (4 Cores, 8 GB RAM, 150 HDD) 1 ADFS Proxy Server (2 Cores, 4 GB RAM 100 HDD) 1 AADSync Server (2 Cores, 8 GB RAM 150 HDD) CTS Support for .1 FTE per environment Monitoring for availability	3 ADFS Server (4 Cores, 8 GB RAM, 150 HDD) 2 ADFS Proxy Server (2 Cores, 4 GB RAM 100 HDD) 1 AADSync Server (2 Cores, 8 GB RAM 150 HDD) CTS Support for .15 FTE per environment Monitoring for availability
Est. Cost: $1,590 per month	Est. Cost: $2,560 per month

CTS must manage ADFS and AADSync Services due to high level privilege on the EAD for these services and access to a GC for every domain on the forest; requires Enterprise Admin rights.

Azure Active Directory

- Released for General Availability in April 2014 as a service
- Three licensing levels: Free, Basic and Premium
- Has existed as the directory for O365 for many years; limited to a single instance per tenant
- Provides a single, cloud identity store
- No passwords are stored in AAD but allows cloud-based password reset of EAD passwords
- Wizard based federation with over 2,000 cloud providers; 10 per user free
- Allows synchronization of multiple identity stores to single instance (Premium)
- Multi-factor authentication available for both cloud applications and on premise resources (Premium)
- Includes FIM and FIM CALS (Premium)
- Allows internal applications to be presented as cloud applications (Premium)
- Developing Administrative Units for delegated administration similar to existing domain and OU structure in EAD (Premium)

CTS Tenant Design

- A single shared tenant for AAD and O365
- A single synchronization engine - AADSync
- A single authentication connection – ADFS
- A process for managing the shared pool of licenses though groups
- A process to track agency license usage similar to daily replication reports
- CTS holds Global Administration role in tenant and delegates to agencies through RBAC.

Single Tenant Benefits

- Single ADFS and AADSync Server for all of EAD with existing high availability for ADFS and Proxy
- Migration path for Exchange and Lync
- Single Identity Store for Cloud Services
- Global Address List maintained
- Collaboration between agencies simplified
- Ability to publish and share cloud applications and on premise shared applications to the cloud securely

Single Tenant Challenges

- Agencies who have purchased O365 licenses are keenly interested in using the SharePointOnline and One Drive now
- CTS would have to be responsible for global O365 SharePoint administration including creating site collections and provisioning storage
- CTS holds global administration role in the tenant
- Future functionality for delegation is still in development and unknown at this time
- Azure Active Directory and the 0365 Government Community Cloud are evolving rapidly – moving target

Multi-Tenant Benefits

- Agency controls global administrator role in tenant
- Agency maintains their own license pool
- Agency maintains own identity store limited to their agency

Multi- Tenant Challenges

- Only a single O365 tenant can be associated with an AAD Directory; CTS manages connection and servers
- Each tenant requires a unique ADFS and AADSync Server for SSO and automatic synchronization; requires additional infrastructure
- Only a single hybrid connector can be configured from Exchange and Lync to a single O365 tenant for migration
- Global Address List cannot be synchronized to multiple tenants
- Collaboration and sharing of applications with other state agencies (both cloud and on premise AAD hosted) would be difficult, require additional license purchase, or be impossible.
- Unable to synchronize unique accounts to multiple tenants
- Scatters state identities to multiple identity stores; less secure.

Challenges for Both

- External Access for customers to SharePoint Online is unclear.
  - May require additional licenses or PAL license
  - May require manual maintenance of accounts
  - SAW integration and account synchronization is not in place and would require time to investigate options
- Administrative responsibilities for services both for CTS and Agencies require more investigation and potential training
- Features available and delegation needs more time to investigate and match up to agency business needs
- Migration path requires time to plan and implement; not all agencies are ready